KDHE Computer Security On the Alert for Trouble

Hackers post between 30-40 new hacking tools on the Internet each month, and the numbers continue to increase daily, according to Norma Jean Schaefer, KDHE Information Security Officer in Information Services (IS).

The job of protecting KDHE computer users and systems from these small programs with huge destructive potential falls squarely on the shoulders of Schaefer and her staff. Schaefer conducted her quarterly information security awareness training for KDHE staff last week, and the message was clear – be vigilant in protecting your office and home computers against the growing threat of identity threat.

"The unsophisticated hacker can search the Internet, find and download exploitable tools, and then 'point and click' to start a hack on your PC at KDHE or at home when you're connected to the Internet," Schaefer said. "If you store valuable personal data on your PC, either at work or home, develop a plan to protect it from hackers."

With identity threat a growing crisis; Schaefer emphasized the need to control access to PCs through proper password generation and protection and to review the methods personal or confidential data is stored on portable storage devices, which are easy targets for theft.

Norma Jean Schaefer, KDHE Information Security Officer, coaches agency staff on best practices to keep data safe and prevent identity theft.

Schaefer said 823 new worms and viruses were identified in the fourth quarter of 2004, up 169 cases from the third quarter. In 2004, Information Security Services, a world leader in Internet security systems, monitored more than 149 million security events worldwide. KDHE experienced just more than one million events in 2004.

One of the main goals of the agency wide seminar was to make KDHE staffers aware how to help Schaefer and her staff fight the cyber intruders and keep network systems running virus free, and to protect individuals from identity theft.

While KDHE has invested in technology designed to block suspicious e-mails and file transfers, Viruses can still infect any office or home computer and network by infiltrating via floppy diskettes, CD-ROM, USB Drives, infected e-mails and Internet Web sites.

-Continued -

Methods that can work to prevent introduction of a virus into a PC are:

- Scan floppies, USB Drives and CD-ROMs at first insertion into a computer;
- Install virus protection software, and keep it current with Internet downloads;
- Install a firewall on the network, and home computers. PCs connected 24/7 to DSL or cable-modems without firewall protection can be hacked just as easily as networks;
- Scan e-mails before opening;
- At KDHE, advise Information Systems if you suspect a file might be infected.

Schaefer emphasized the when in doubt call the Help Desk or IS to report suspicious e-mail or computer activities. While IS works around the clock to monitor, and safeguard the KDHE cyberworld, she said "computer sec_rity is not complete without 'u'."